1

## COMMITMENTS IN SIGNATURES

3	The present invention provides methods and apparatus
4	for generating a TCR-commitment having properties
5	differing from the properties of a regular commitment.
6	It provides solutions to the problem of packet
7	authentication for multicast and other scenarios
8	requiring fast, compact digital signature/commitment
9	for E-commerce protocols. It also provides a
10	relatively high level of security guarantees required
11	for packet authentication in a way that can handle
12	multiple independent flows, produces authentication
13	fields of fixed size, works in the fully unreliable
14	setting, does not require any packet delays and has the
15	additional property of being able to withstand and
16	smooth over irregular processor loading and bursty
17	packet output rate. In an embodiment, it uses a hybrid
18	approach consisting of the commiter/signer/bidder
19	creating a certificate for the public key of an
20	efficient k-time signature scheme using a regular
21	signature key. The commiter/signer/bidder then signing
22	up to k messages with the private key corresponding to
23	k-time public key. The time consumed to compute a
24	public key signature is amortized over k signatures.